AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("~~—~~") being deleted:

1. (Currently Amended) A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

~~automatically~~ transmitting all requests to send data; and

storing in a buffer data relating to requests which identify a destination host not in the record.

2. (Original) A method according to claim 1 wherein the record is established by monitoring identities of destination hosts to whom requests have been transmitted during a second time interval, which precedes the first time interval.

3. (Original) A method according to claim 2, wherein the record contains a predetermined maximum number of destination host identities, the maximum number being defined in accordance with a policy.

4. (Previously Presented) A method according to claim 3, wherein the policy additionally defines a maximum number of destination host identities not in the record, to whom requests may be legitimately transmitted in accordance with the policy.

5. (Previously Presented) A method according to claim 4 further comprising the step, at the end of any given time interval, of deleting from the buffer data relating to requests transmitted during the given time interval in accordance with the policy.

6. (Previously Presented) A method according to claim 5 further comprising the step, at the end of the given time interval, of updating the record to reflect identities of hosts identified in requests which are transmitted in accordance with the policy during the given time interval.

7. (Previously Presented) A method according to claim 6 further comprising the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with the policy.

8. (Previously Presented) A method according to claim 1, wherein the stored data is offered in the buffer and includes a copy of a socket created to send data in accordance with a request.

9. (Original) A method according to claim 8 wherein the socket enables identification of at least one application program at whose behest the socket is created.

10. (Previously Presented) A method according to claim 1 further comprising the steps of:

determining the value of parameter ("slack") based upon a number of successive time periods that pass when no new requests are made to send data from the first host to hosts not in the record; and

when slack exceeds a predetermined value, allowing un-impeded passage of data from the first host to destination hosts not in the record.

11. (Original) A method as claimed in claim 10, wherein slack is determined based upon the number of successive time periods for which the buffer is empty.

12. (Original) A method as claimed in claim 10, wherein slack has a predetermined maximum value.

13. (Previously Presented) A method as claimed in claim 10, wherein the value of slack is decremented each time an un-impeded passage of data from the first host to a destination host not in the record is allowed.

14. (Original) A method according to claim 10, wherein said time periods are of equal duration to at least one of said time intervals.

15. (Previously Presented) A method according to claim 1 further comprising the steps of monitoring the rate of increase in the size of the buffer, and

in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a virus warning.

16. (Previously Presented) A method according to claim 1 further comprising the steps of monitoring the increase in the size of the buffer per time interval, and

in the event that the increase in the size of the buffer in any given time interval exceeds a predetermined size, generating a virus warning.

17. (Previously Presented) A method according to claim 1 further comprising the steps of monitoring the size of the buffer, and

in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a virus warning.

18. (Previously Presented) A method as claimed in claim 1, further comprising the step of varying with time at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record.

19. (Previously Presented) A method as claimed in claim 18, wherein said at least one parameter is varied as a function of the time of day.

20. (Previously Presented) A method as claimed in claim 18, wherein said at least one parameter is varied in response to a perceived threat level.

21. (Previously Presented) A method as claimed in claim 18, wherein said at least one parameter is changed between a first set of values and a second set of values at a predetermined rate.

22. (Previously Presented) A method as claimed in claim 21, wherein at least one of the values of said at least one parameter is randomly changed according to a predetermined probability distribution as a function of time.

23. (Previously Presented) A method as claimed in claim 1, further comprising the step of determining at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record by performing an automated search on a set of data indicative of normal network traffic.

24. (Previously Presented) method according to claim 1 further comprising the steps of:

receiving a request to send a multiple recipient email from the first host;

determining the value of a parameter ("mslack") based upon the number of successive time periods that pass when no multiple recipient emails are sent from the first host;

if mslack exceeds a predetermined value, allowing un-impeded passage of the multiple recipient email.

25. (Original) A method according to claim 24, wherein the multiple recipient email is allowed un-impeded passage if mslack is greater than or equal to the number of intended recipients of the email.

26. (Original) A method as claimed in claim 24, wherein mslack is set to zero after the multiple recipient email has been sent.

27. (Original) A method as claimed in claim 24, wherein mslack has a predetermined maximum value.

28. (Previously Presented) A method according to claim 24, wherein said time periods are of equal duration to at least one of one or more time intervals.

29. (Previously Presented) A method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host:

over the course of a first time interval, monitoring creation of sockets within the fist host to identify destination hosts identified therein;

comparing identities of destination hosts monitored during the first time interval with destination host identities in a record; and

storing data from all sockets which identify monitored destination hosts not in the record.

30. (Original) A method according to claim 29 wherein the stored socket data at least enables identification of the destination host identified therein.

31. (Original) A method according to claim 29 wherein the record identifies a maximum number of destination hosts, the maximum number being determined in accordance with a policy.

32. (Original) A method according to claim 31 wherein the record is established by monitoring creation of sockets during a time interval preceding the first time interval.

33. (Previously Presented) A method according to claim 31 wherein the policy additionally specifies a maximum number of sockets, each identifying a destination host not in the record, to be legitimately created in any given time interval.

34. (Original) A method according to claim 33 wherein at the end of a time interval, socket data containing identities of destination hosts in respect of whom sockets have legitimately been created is deleted.

35. (Original) A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host.

36. (Original) A method according to claim 35 wherein packets having a designated destination IP address are stored.

37. (Original) A method according to claim 36 further comprising the step of establishing the predetermined IP address from the stored socket data.

38. (Original) A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing incoming packets to the first host.

39. (Original) A method according to claim 38 wherein packets having a designated source IP address are stored.

40. (Original) A method according to claim 39, further comprising the step of establishing the predetermined IP address from the stored socket data.

41. (Original) A method according to claim 29 wherein socket data is stored in a buffer.

42. (Previously Presented) A method according to claim 1, wherein the step of automatically transmitting all requests comprises transmitting the data related to the requests.

43. (Currently Amended) A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

~~automatically~~ transmitting all requests to send ~~data regardless of a result of said comparing;~~ data; and

based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record.